The Protection of the Digital Medical file Between Privacy and Information Security

Amal Fawzy Ahmed Awad

Head of the Information Technology Unit, Faculty of Art Education,

Helwan University, Egypt

Amal_fawzy@fae.helwan.edu.Eg

Abstract:

Health care practitioners throughout the world are keen to digitize and use health information technology solutions such as electronic health records to improve patient care quality, although technology has played a key role in the development of this area. But cyber-threats can cause complete paralysis and damage to medical systems, how will they address all legal and social challenges? the application of ongoing review policies to ensure the quality of the protection and privacy of information security has become necessary. The transition to digital is no longer a luxury, no choice, but a challenge today and a necessity for tomorrows and the currency of the future economy.

Keywords: Medical; Electronic; Data Security; Digital Privacy; laws.

Introduction

Electronic medical records (patient's file) do not differ much from traditional paper records in their function and purpose, but they are completely different in nature, characteristics, possibilities of use and benefits, they are a central point poured into it and many channels of information related to providing health care to the patient are dissected, and they are also precise content and accessibility features through integration with the various sources of information through systems e management companies, institutions and information networks, which led to use by extension to the evolution of the idea of decentralization and communication of information between more than one hospital and medical institution, but the evolution of the case even further through a network international Internet , which provided communication between users of doctors and patients from different countries of the world, and who are separated by thousands of miles are gathering one network information .

It has been defined by the American Society for Health Care Management Information and Systems as a "medical record in digital format", and the patient's electronic file contains all the patient's personal and administrative information, diagnostic information, history, vital indicators, treatment measures are taken, approvals of these procedures, the results of medical analyzes and x-rays if It is an information repository that includes all patient information and depends on the computer with all its advanced capabilities such as storing information, processing and transmitting data through information networks and digital communication media. [1].

Chapter one: Converting the patient's file to digital [2]

First: Organizing the patient's digital file

The conversion of the patient's file to the digital and electronic organization of health is the application of technology and information development in the medical field. The basic applications of medical informatics find themselves first in the electronic medical file whose accreditation has become mandatory in many countries, and it is one of the important conditions for the development of the health sector and health services, being the record that contains sensitive medical personal information   [3] Relating to the patient and requiring protection.

This application may take place at multiple levels, for example, if it is within the doctor's office, for example, or within a specific hospital, including all its health departments and employees, from the medical structure to the administration, or within a specific city (for example, the Planning and Quality Center for Medical Services in Dubai Healthcare City, which means establishing a system Integrated medical in the city), or it may include certain sectors within the state, such as connecting hospitals to the National Social Security Fund, or it may include the entire lands of a specific country, for example when the US administration launched a project in 2005 to create a nationwide network of electronic health

records (EHR) Within ten years, or when it launched the C liters since 2002 , a national program of information technologies specialized decimal in the medical field, or may include the world as Microsoft finally announced its plans for the site Health Vault website It is a new service for storing, managing and obtaining patient medical information[4] It works as an encrypted service on the network that provides the ability to collect medical records data from multiple sources, such as insurance companies, health service providers, and some medical devices (such as blood pressure measuring devices, for example). And intend to google Also "provide a similar service.[5]

Second: The components of the patient's digital file:

The association of the patient's electronic file and the integration of its content with other subsystems within hospitals and medical centers can now provide health care professionals with any information, such as information about patients in an integrated and coordinated manner such as treatment, medical history, results of practical examinations (blood, hormones, Enzymes - digital images of body parts (X-ray and CT scans, complex numbers) Linking the patient's electronic file to the system of entering medical orders such as: (medical examinations - prescriptions).

Third: Mazza O the file Digital's patient:

The electronic medical file of the patient has many advantages, which makes each medical institution not to abandon its application to get rid of paper that has many drawbacks such as slow movement, difficulty retrieving its information, and the large loss of data. This and health record mail is the convergence of all the systems point, to contain the medical file mail on all medical findings and diagnoses and treatments performed for the patient and the drugs given to him , also provides an opportunity create communication between individuals and teams to provide health services from doctors, nurses, technicians and administrators , and containing medical records electronic many of the information that contributes to the development of scientific research, and the people who provide them with medical reports, administrative and statistics that serve the hospital 's activities , and provides the possibility of linking hospitals with each other , and helps to improve the accuracy of data recorded in the health record , and helps improve the quality of health care provided to the patient by providing the necessary information in a timely manner , Wei raise the efficiency of health services and the provided costs by speed in the exchange of information .

Fourth: Disadvantages of the patient's digital file: [6]

Also computing cloud t carries many of the risks, which include:

The possibility of compromising the privacy of personal health information (PHI); The information of health that is detected by individuals not authorized them, or access to it is not illegal, or tamper with them, or erased maybe its effects

devastating on the health of the patient or even on his life. Q according to what is mentioned, 94% of US health organizations had previously been the process of at least one breakthrough over the past years and almost 20 million electronic medical files have been breached his privacy [7] During the past two years in the USA.

Fifth: What should be taken into account in the patient's digital file: 1 / The users' need for information: It is one of the main challenges facing the process of developing systems and converting them to digital, and experience has proven that successful digital medical systems are being developed either by or with the help of doctors and specialists In health care and two projects, where the rapprochement between the developers of these systems and between doctors and specialists provides a deeper understanding and a more comprehensive awareness of what the medical care process requires in terms of the nature and characteristics of information and how to use it.

 2 / Ease of use: Systems developers have to consider several points, the most important of which is the nature of doctors, their needs, and the difference between them and professionals in the field of information technology and network security.

3 / Standards [8]: It helps to increase accuracy and complementarity between the various institutions, reduces errors and costs, increases the value of scientific research, and increases the integration of development efforts and investments.

4 / social and legal challenges: These are challenges related to the extent of privacy and security of electronic medical information. The more easily this information is accessed, the more important it is to establish more security and privacy rules that govern the use of information and the right to access it.

• Costs vs. Features: These are the most important economic challenges for the electronic medical records systems industry. The higher the required properties and features, the more costs for their production and provision will increase, and an appropriate balance must be reached between them. [9].

Chapter two: Digital privacy and information security [10]

 Although the terms "privacy" and "security" are often used interchangeably, they are different disciplines. Information security and privacy are two distinct disciplines linked together. For proper privacy protection, proper security mechanisms are needed. Given the sensitivity of personal information collected, used, and shared in the healthcare environment, it is important to define and implement appropriate security mechanisms that protect health data and the privacy of individuals. [11]. Security and privacy requirements must be defined, the selection and implementation of the necessary controls during the stages of the system development cycle, and security and privacy protection updated as needed. It is also important for individuals to cooperate in information security and privacy organizations to manage security risks and protect privacy.

First: What is the difference between security and privacy? [12]

In this technology-era digital era, security and privacy must be a major requirement. As everything became interconnected and easily accessible, most Our data and information Personality is available for piracy and security threats, so everyone needs protection and privacy, especially for people working in communications. But most of us don't know what the difference between security and privacy is.

Unfortunately, security breaches have become very common, according to the 2017 Internet Crime Report, more than a billion personal records were stolen, and in the United States alone more than 100 million Americans had their medical records stolen in 2016. And if these statistics indicate something, they indicate the urgent need to enhance security and privacy.[13]And before going into the question of the difference between security and privacy must be defined each of them separately:

Safety: A condition that indicates personal freedom from external forces and freedom from potential errors and threats. Like the home security system that protects your family, data security protects personal data and information by protecting your passwords and documents. An example of security is anti-virus software on your personal computer that protects your computer and makes your files safe. With the development of technology, strict measures and measures have been put in place to protect digital data from unauthorized access and protect this data from Internet hackers and cybercriminals, and all security measures try to address one of the security goals: protecting confidentiality, preserving the integrity of information assets, and enhancing the availability of data and information.

Privacy: It is a person's right to be free from prying eyes. It is one of the basic principles of human dignity and includes confidentiality and protection of sensitive information such as personally identifiable information.[14] Hence, it is impossible to implement a privacy program without a security program.[15th]

And despite the similarities between the two terms and the interrelationship between the two thorny, but safety is the case of personal liberty and freedom from potential threats, but privacy is freedom from unwanted attention and intrusion on privacy. The difference between privacy and security is in:

Objectives: Secret security objectives, integrity, and availability and protect your confidential information and data from unauthorized access. As for privacy, it refers to the rights of individuals and institutions regarding personal information.

Programs: A security program refers to a set of protocols and regulations established for all confidential information and resources that the organization collects and owns, and focuses on data and information rather than personal information for individuals. The privacy program focuses on protecting personal information only, such as login and passwords.

principles: Security principles include protecting confidentiality, preserving the integrity of information assets, and enhancing the availability of data and information. The privacy principles set out the rights of individuals and organizations about personal information.

Interdependence and dependence between the two terms: Security can be achieved without privacy, but privacy cannot be achieved without security. [16]

Legislation that defends privacy is based on its definition as an important value for members of society. Because of the novelty of the issue of digital privacy, the legislative frameworks differ from one country to another according to the developments experienced by each country, its legislative philosophy, how to apply the laws and transformations that society is going through, and the ability of each country to adopt an amendment to its laws based on new issues that are outside its legislative framework [17].

And the privacy protection of media laws concerned with the transfer of information either over the Internet or phone or even mail also includes maintaining the confidentiality of information in their records of individuals, such as financial or health information. It must also guarantee their private data that is circulated through browsing and communicating on the Internet.

This has resulted in the use of the Internet different challenges to the topic of privacy protection, and the different types of laws concerning privacy in the digital space are ranging from protecting email, imposing restrictions on the publication of social media data, and monitoring the activity of the Internet browser and violations of the saved data. Here are the different types of digital privacy laws:

Data Protection Act: It is imposed on companies providing Internet services that store digital information for their clients from publishing this information or sharing it with other parties without the benefit of the customer [18].

Communications Control Law: Internet communication control, which is in the workplace, in public places, or even at home, is restricted.

Internet Crime Protection Law: It prevents identity hijacking or email theft and everything related to protecting personal data that individual shares while using the internet.

Tha Nya: How works security and privacy together?

Security measures are needed to protect the privacy of individuals. Know the techniques and tools that support the privacy technologies enhanced privacy, and often are made up of techniques for security protects use the privacy of individuals. You can use the techniques of enhanced privacy to perform functions such as enabling access to data and use it on some appropriate internally, and to prevent disclosure is not appropriate for the data externally. However, just use the mechanisms of security to help the efforts of privacy, some measures Privacy help also in the efforts of security.

Chapter Three

Legislative models to protect the security and privacy of the digital medical file [19]

First: a brief overview of legislation data some countries in the field of security and privacy of data digital health: [20]

The development of informatics has developed the legal framework for electronic exchanges. Legal protection for health data comes mainly from general texts in domestic and international law, and from the legal standards established by countries and managed by global conferences to organize an electronic activity, we can provide a very brief overview of the legislation in some countries as follows:

In Lebanon:

There are no special laws or regulations related to the protection of medical records and electronic data, but rather general principles contained in the following texts:

Article 7 of the Medical Arts Law No. 288 Date of 22/02/1994 amended by Law No. 240 Date of October 22, 2012, stipulated that the secret imposed on professional external Labib medical assistant is the body of Allen General Zam, and exempted from it in exceptional cases such as contagious diseases. .. Note that this obligation has moved from being a medical secret to becoming an information secret that starts from gathering information to investing it on the network, whether by the medical body or the agencies responsible for storing, transporting and investing it.

Article 29 of the same law stipulates that the medical file must be kept in the patient's clinic and in the hospital under the responsibility of the department head and that it should not be handed over except to the patient or his legal representative under a power of attorney expressly authorized by him, or to the physicians and researchers, or to a third person bound to professional confidentiality. The treating physician or researcher is entitled to take advantage of the medical files under his responsibility to serve the scientific development provided that the names of his patients are not disclosed and the condition of maintaining professional confidentiality ... The investigating judge or the judicial police have the right to inspect the doctor's office or the medical department and lay hands-on medical documents in the presence of one of the council members The union. The doctor is then not entitled to oppose the inspection procedures. And the judicial authorities and health and union doctors to obtain a copy of n any medical file to be the subject of a complaint and investigation.

Item 9 of the same article also states that doctors and health institutions must keep medical files for at least ten years unless the patient's interest requires that this period be extended.

As for Article 579 of the Lebanese Penal Code, it stipulates that any person

who unlawfully reveals a secret who reached his knowledge by his profession or art or who uses it for his benefit or the benefit of others will be punished.

And Article 264, Clause 1, Principles of Civil Trials, Legislative Decree No. 90, dated 16/9/1983, stipulates that no information or facts that have reached the lawyer or doctor's knowledge ... while practicing his profession should be disclosed.

Articles 8, 12, and 17 of the Patient Rights and Informed Consent Law No. 574 of February 11, 2004 deal with the right to respect for personal life, the confidentiality of patient-related information, the limitation of information given to guarantor institutions on the information necessary to pay for medical costs, and the right of the patient's expected family to obtain the necessary information After his death, he has the right to view his file to know the reasons for his death.

As for Articles 21, 23, and 24 of the Human Genetic Examinations Law No. 625 of 11/20/2004, it has organized the preservation of the results of the laboratories of DNA And its inclusion in an information network, because of the nature, severity, and confidentiality of these complex checks (Article 7) and prohibited any public or private access to them that allows the identification of the person with the record.. These texts have referred the method of preserving the file to the rules stipulated in Articles 7 and 29 of the Code of Arts Medical.

Thus, we see that there are no legal details related to informational activity or health electronic records and data except for laboratories DNA and, in general, as it are up to health institutions according to their development and implementation of international standards.

In America:

The most famous laws: A federal law that sets patient privacy standards in 50 states The federal Health insurance portability and accountability Act HIPAA)) Put into effect on April 14, 2003, and applied to the medical records maintained and managed by the suppliers and specialized institutions, health plans, and health clearing if their documents are electronic. In short, it regulates the collection, management, and transmit medical information funded the accent and the right of the patient's access to its records. But it is not comprehensive, and a wide area of activities remains in need of directions to ensure protection. And the first case that the Ministry of Justice considered in the application of HIPAA The year 2007 was a claim of theft of electronic medical records related to 1130 patients at the Cleveland Clinic, where one of the employees of the institution stole and sold files to a criminal organization that had already obtained $ 7 million in sickness insurance Medicare.

As for the American Health System Reform Act of 2009, the electronic medical file gave special attention and systems to protect its information and the way it is used by all parties to the medical relationship and gave the patient many powers as basic rights to him, and involved him in making the decision and making it the

focus of treatment, and forced all users of health information to exchange it electronically, He organized its protection and the way it is used from all sides of the medical relationship, and gave the patient many powers as basic rights, and involved him in making decisions and making him the focus of treatment.

In Canada :

A law on the protection of personal data and electronic documents is a model law for the Canadian Standards Association.

In Europe :

Directives and recommendations of the European Parliament (especially the recommendation of October 24, 1995) on the protection of persons on the subject of processing information of a personal nature and freedom to transfer data, including medical and genetic information, as stated by the European Council of Ministers in 1977, and this recommendation was modified according to Directive No. 58 of 2002 about Private life and electronic communications, then Directive No. 24 of 2006, on data conservation.

In France:

Decree No. 960-2007 dated May 15, 2007[21] Measures and standards for the confidentiality of medical information saved electronically or transmitted by electronic means.

 The text of the law on informatics and freedoms[22] In its articles 38 and 39, the right to enter personal medical data and the patient's right to object to the exchange of his information for legal reasons. Article 1110-4 provides clause 3 of the Public Health Law [23] that the patient who is carefully present in the medical team in a health institution, the information concerning him and his will is under the custody of the team as well as if the matter concerns a group of therapists in a clinic or medical center. This article provides for the role of the judiciary and the National Informatics and Liberties Authority   CNIL In measures to ensure the confidentiality of medical information and the penalties for violating it. Patient satisfaction remains legally and expressly required when storing and hosting information hébergement According to Article 1111-8, Clause 1 of the Public Health Law, and among the constants of the National Informatics and Liberties Committee CNIL The sharing of the patient's medical information via the Internet to coordinate the treatment is conditional upon his prior express consent.

As for the legal protection standards for health data , in general, and in application of "legal and regulatory texts to protect the privacy of health electronic data, in the West, especially in North America, institutions have been established that prepare and manage electronic medical records and information systems and programs that allow the processing and management of health information electronically, adopting protection policies and standards derived from Laws, regulations, and technical expertise: Hospitals, medical centers, and infectious disease centers have also applied the principles of legal protection for private life starting with the

issuance of a declaration that adheres to its application that includes how to collect, analyze and archive personal health data, appoint those who do so from the staff of the center and the extent of their responsibility, and show details Practices and the full rights of the patient and what they can or refrain from spreading or sharing with others without the patient's permission and for whom and how and what medical data is legally protected or not protected With more protection for the privacy of its data.

Second: International experiences in legislation protecting digital privacy [24]

International treaties included articles that preserve the individual's right to privacy, and to ensure that he is not arbitrarily or unlawfully subjected to interference in his privacy, family, or home affairs or correspondence, provided that the law protects him from such interference or prejudice[25].

The European Union member states have also contributed to legislating their laws to protect digital privacy, and the European Union has contributed to some of the criteria that were within the European Convention on Human Rights, which stipulates in Article 8 on privacy that :

1-   Any person has the right to have respect for his personal and family life in addition to his home and correspondence.

2-   The state has no right to interfere in this right except under the law and the dictates of necessity in a democratic society, and what affects the national security or public or economic safety of the country or to prevent chaos and what may harm public health and morals or to protect the rights and freedoms of others[26] ".

This has led to the expansion of the concept of privacy despite the differences in the application of the law from one country to another. We find that Spain and Germany have the most strict laws, while Spain is the most European country that registers complaints against a violation of data protection.[27] The most collectible fines against violations of personal data[28], As for the countries of the Asian continent, Singapore has made in 2012, the enactment of laws for the protection of personal data gives the protection period of ten years after the death of the person [29], And South Korea's law is also among the strongest in Asia, as one of the provisions of the law provided for the protection of the individual's image and voice [30].

And many Latin American countries have enacted laws to protect the privacy of individuals, guided by the directives of the European Union countries, to open up the commercial market with them. In 2000, Argentina enacted its law to facilitate trade between it and the European Union, and the legislation was based on European Union standards.[31].

As for the United States of America, their privacy laws are incomplete and suffer from legislative poverty. Some laws cover financial data such as bank accounts and addresses. [32] Another health-care provider also has legislation that obliges

sites that collect information about children under the age of 13 to develop a privacy policy on how to verify the consent of a parent or child's official when children publish their data.[33] There are also unspecified contributions within a legislative framework, for example, American stores have a self-protection policy to protect their customers, but prosecution in case of violation will not be met by any legal penalty and the consumer will find a solution only by not buying from the store.

And some institutions have adopted drafting laws for digital privacy following developments in digital privacy. In 2010, the US Federal Trade CommissionFTC A report reveals consumers' right to prevent websites from following their internet usage behavior [34]. The focal point of this draft law is that it restricts internet browsers by including a non-tracking function, and it is also proposed that commercial entities disclose the current status of the personal data they have collected and with whom they have shared.

In January 2012 the European Commission proposed a data protection legislation that makes an individual the right to ask Internet service providers to erase his data that can appear in search engines. The legislation is called the Right to Be Forgotten, and the proposed law tries to allow users to require companies like Twitter and Facebook to delete their private data as well as Google to prevent this data from appearing in their search engines.

Chapter Four: Digital security [35] and health care

Represents an Internet connection need to conduct many activities that may represent part of the use of electronic health records and health data for patients, and is the exchange of patient data electronically and submit claims electronically, and generate electronic records of requests for examination of patients, medical prescriptions are all electronic examples of activities carried out over the Internet and relies On cyber security practices to protect systems and information.

first: the importance of protecting electronic health records for patients:

it systems that keep sensitive and confidential data of individuals and process them are an attractive target for cybercriminals. therefore, it is extremely important to protect patients' electronic health records, which are:

ensuring availability of health care services: any interruption in health care services may have a disastrous effect on patient health.

keeping intellectual property rights secure: research laboratories create and host assets in the form of highly valued intellectual property for stakeholders.

preserving reputation: the reputation of a health facility is an inherently indispensable asset. any electronic attack, regardless of its nature, will harm credibility if it is publicly disclosed.

Second: Information security standards in health care:

Information security is the protection of data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information security is achieved by ensuring the confidentiality, integrity, and availability of information. Security, based on the above-mentioned legislation, in the electronic age, which means the safe handling, storage, transmission, and use of information, has three fundamental aspects:

- Preserving the confidentiality and confidentiality of the information   La confidentialité (): It means preventing unauthorized people from accessing information that identifies the patient's identity. The control of these secrecy laws and regulations and a means to protect the most effective is the coding and electronic signature and identification of the user in various ways and Â Maly regulates admission. The confidentiality of information requires responsibility for its preservation, determining the goals of collecting, using, publishing, and preserving it transparently, and with the consent of individuals to do so, the accuracy and timeliness of this information, measures for its protection, and the right of individuals to enter it, objection and claiming violations.

- Safety Information (L'intégritéA: It means that the information is complete and that its amendment or disappearance is prohibited. This happens, for example, when the doctor notices that the device stopped with a malfunction for a long time or that information has been lost or erased, which causes medical errors, but it allows modifying some data if it is found to be incorrect or if it changes, with the consent of the patient and the doctor.

- Accessibility to information (L'accessibilité): Means ensuring access to information realized with the consent of the patient since he either used outside the medical goals or medical research, it requires clear approval only if the law allowed it (statistics of infectious diseases) and the access to electronic information through encoding or electronic signature and the definition of the user and allow access.

Chapter Five: Preventive measures for the security and privacy of the digital medical file [36]

First: Preventive measures for information security in the field of health care:

The medical file, paper and electronic, accurate and organized according to rules, is the most effective medical management tool developed daily by the disposal of doctors in all their specialties, for their benefit and the interest of their patients, because it improves and supports their medical performance. It also constitutes a legal document describing in detail all the medical and administrative work that the doctor performs during his treatment of his patient, and insurance companies rely on them to make their decisions without relying on the doctor's statements and explanations. Therefore, preventive measures for information security in the field of health care are divided into administrative, material, and technical measures. These are examples of each:

Administrative preventive measures:

Continuous assessment of the risks to the health IT environment.

Continuous evaluation of the effectiveness of preventive measures related to electronic health information.

Detailed processes for displaying and managing electronic health information.

Training employees in using health information technology to adequately protect electronic health information.

Reporting security breaches and ensuring continued health information technology operations.

Physical preventive measures:

Office alarm systems.

The allocation of closed offices containing computer equipment in which electronic health information is stored.

Appointing security guards.

Technical safeguards:

Securely install computer equipment (such as virus and firewall scan), and approved applications and technologies that store or exchange electronic health information.

Define controls for access to health information technology and electronic health information (such as authorized electronic accounts).

Encryption of electronic health information.

Health Information Technology Audits.

Back up health information technology (such as making regular backups of electronic health information to another computer server).

Second: Prevention of cyber attacks

Privacy focuses on an individual's ability to control the collection of his or her identity data [37] it may be used, published, and preserved, and privacy workers may differ on the role that consent should play in promoting trust and improving privacy, but it plays an important role in protecting health information. By adopting a comprehensive approach to privacy, government agencies and entities that create and use new health technologies can improve the health of the public, while preserving the confidence of individuals and meeting their expectations for individual privacy, and information privacy and security are of paramount importance for all individuals, government agencies, and private sector organizations. Protecting Information in the health care sector j characterize the importance of greater than any other sector, Q some actions can be taken to protect health institutions from cyber-attacks, including:

Reject employee requests to take laptop computers with unencrypted patient data home.

Removing hard drives from old computers before disposal.

Do not send any email containing health information to patients if they are not encrypted.

Ensure the presence of the computer server in a room that only authorized

personnel can access.

Sensitize health institution staff to the need to randomly monitor their access to the network.

The enterprise's electronic health records server is periodically scanned for viruses and malware.

Findings and recommendations

To maintain the security of health information, the following should be considered:

There will be the globalization of privacy, in which the principles of the practice of information will be relatively consistent across the world, with increased accountability and increased enforcement efforts. Besides, health care data is expected to be part of this globalization as healthcare companies expand their borders, hiding any geographical lines.

Expect the emergence of an economy of open information that permeates across geographic borders, as more people see data, so it will be necessary to increase transparency and improve health care consumer education to maintain patient confidentiality.

Deselected data will play a more prominent role in protecting patient privacy, allowing the free flow of data for innovation and research.

More health care institutions should be encouraged to adopt a method of removing identifiers and establishing appropriate use of applications in which personal health data can currently be used, for the benefit of both individuals and the health care system..

Although countries that have legislation that protects the privacy of their citizens from exposing their data to theft or spying or exploiting them for commercial and advertising purposes, these legislations are not clear and they have many legal loopholes as they relied on old standards and did not cover all cases that oppose digital privacy.

Governments that control citizens under the protection of national security and combating criminal and terrorist organizations may not have laws that maintain privacy.

A law must be legislated to preserve digital privacy that does not conflict with freedom of expression and privacy as stipulated in the constitutional articles, and this law should obligate companies that provide Internet and telecommunications services not to keep personal data without the owner's knowledge. All illegal oversight programs must be criminalized, whether by government agencies or private companies.

The most important thing that may preserve the privacy of digital individuals is not only legislation in law, but also ensuring its application in addition to its ability to amend based on any violations that may affect digital privacy.

It is recommended to encrypt all information stored in the medical file or during

the process of its exchange.

Keep the keys of the encrypted information in a safe place elsewhere.

Apply strict policies to control access to health information and data.

Apply continuous review policies to ensure the quality of the protection and privacy process

The necessity of training health professionals in our country on the correct use of informational devices and programs, especially in managing electronic medical records, and making them aware in the practice of their benefits and risks, the rights that regulate their use and protecting their users, and the privacy of sensitive information that they contain.

Establishing new and comprehensive legislation for public health and patient rights, and establishing a national informatics and liberties authority vis-à-vis the french institution that organizes and sponsors its affairs. Switching to digital is no longer a luxury or a choice, but rather a challenge today and a necessity for tomorrow and the currency of the future economy.

References:
Books:
Data Protection Laws of the World, Downloaded: 7 June 2020.
Theses
Osama Ahmed Attalla Is the Legal Protection of Digital Privacy Enough In Egypt "? Protection of Digital Data Privacy ", A Paper Submitted For the Conference of Cyber Crimes, National Institute of Intellectual Property April 2020.
Reports:
FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers - Federal Trade Commission.
FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers
Journal article Seminar article
Engineer / Saeed Attalla, What is the difference between security and privacy, Article published on 14/5/2020 on the site:
https://www.arageek.com/l/ What-the-difference-between-security-and-privacy
New standards added by an organization "HIMSS" Focuses on Information Security and Medical Imaging. Article posted on April 25, 2017, on:
https://www.ehealthsa.com/archives/2261
Dr. Ehab Abdul Rahim Ali, Health Information Security Article posted on:
HTTPS://ME.KASPERSKY.COM/ENTERPRISE-SECURITY/HEALTHCARE
Security - Information - Health, an article posted on:
HTTPS://TAQADOM.ASPDKW.COM / Health-Information-Security /, the hottest entry date: 6/28/2020
Dr. Khalil Khairallah, organizing the electronic medical file and protecting its data

in the framework of developing the health sector and health services. DOSSIER MÉDICAL ELECTRONIQUE Posted on: https://www.lita-lb.org/archive/51-dossier-médical-Electronique.html (Last access date: 6/29/2020 ")

Laws:

Personal Data Protection Act 2012 - REPUBLIC OF SINGAPORE.

Gramm-Leach-Bliley Act - Bureau of Consumer Protection.

Children's Online Privacy Protection Act of 1998.

Ø Dcret N ° 2007-960 Du 15 by mai 2007 Relatif À La Confidentialité Des Information's Médicales Conservées Sur Support Informatique the ou Transmises Par Voie Électronique Et Modifiant Le code is De La Santé Publique (Dispositions Réglementaires).

Loi informatique et libertés codifiée par la loi nº2004-801 du 6 aout 2004 pour l'harmonization avec la directive européenne .

Code de la Santé Publique , dernière modification: 1 juillet 2014 .

Internet websites

http.//www.healthvault.com

http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8#sthash.jTiWe8R0.dpuf

https://aitnews.com/2018/05/27/ regulations - general - to protect - data - gdpr /

https://ar.wikipedia.org/wiki/ Law _ Privacy _ Information

https://hi-in-ksa.com/2015/12/20/ rules - data - and magazines - scientific - in - the known /

10.HTTPS://ME.KASPERSKY.COM/ENTERPRISE-SECURITY/HEALTHCARE

https://mobile.emirates.com/MobileTermsConditions/jo/arabic/what_sensitive_personal_data_might_you_require_or_hold.xhtml?lang=en_JO

HTTPS://TAQADOM.ASPDKW.COM / Security - Information - Health / , The hottest date : 28/6/2020

https://www.arageek.com/l/ what - the difference - between - security - and privacy

https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ General Data Protection Regulation: Is Will it be the global standard for data protection?

https://www.ehealthsa.com/archives/2261

https://www.lita-lb.org/archive/51-dossier-médical-electronique.html) Last access date: 6/29/2020 "(

https://www.lita-lb.org/archive/51-dossier-médical-electronique.html

Https://www.salamatech.org/ Privacy - from - perspective - rights - human

Www.globalsign.com, briefed him on 07.03.2019

Www.differencebetween.net, briefed him on 03.07.2019

Www.hiv.gov, briefed him on 03.07.2019

https://linkitsys.com/ar/ File - Patient - Registry - Medical - Patient / Health data security in the cloud internet

https://sitcegypt.org/?p=1425 Digital Privacy Legislation /

https://taqadom.aspdkw.com/ Security - Information - Health

https://hi-in-ksa.com/2013/07/08/

Endnotes

[1] Dr. Ehab Abdul Rahim Ali, Health Information Security Article posted on: HTTPS://ME.KASPERSKY.COM/ENTERPRISE-SECURITY/HEALTHCARE HTTPS://TAQADOM.ASPDKW.COM / Health-Information-Security / ,The hottest entry date: 6/28/2020

[2] Dr. Khalil Khairallah, organizing the electronic medical file and protecting its data in the framework of developing the health sector and health services. DOSSIER MÉDICAL ELECTRONIQUE Posted on:

https://www.lita-lb.org/archive/51-dossier-médical-electronique.html) Last access date: 6/29/2020 "(

[3] What sensitive personal data may you need or keep?

Sensitive personal data includes data about a person's health, religion, and other categories of personal data that are closely protected. Check it out:

Osama Ahmed Attalla Is the Legal Protection of Digital Privacy Enough In Egypt "? Protection of Digital Data Privacy ", A Paper Submitted For the Conference Of Cyber Crimes, National Institute Of Intellectual Property April 2020.

https://mobile.emirates.com/MobileTermsConditions/jo/arabic/what_sensitive_personal_data_might_you_require_or_hold.xhtml?lang=en_JO

[4] http.//www.healthvault.com

[5] Dr. Khalil Khairallah, organizing the electronic medical file and protecting its data within the framework of developing the health sector and health services. DOSSIER MÉDICAL ELECTRONIQUE "Previous reference.

[6] The previous reference.

[7] Check it out: https://www.salamatech.org/ Privacy-from-human-rights-perspective

[8] Medical Information Security Standards: Check it out: new standards added by an organization "HIMSS" Focuses on Information Security and Medical Imaging.Article posted on April 25, 2017, on

https://www.ehealthsa.com/archives/2261

[9] https://linkitsys.com/ar/Patient-file-medical-record-for-patient/Security of health data in the cloud

[10] Osama Ahmed Attalla Is the Legal Protection of Digital Privacy Enough In Egypt "? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes, National Institute Of Intellectual Property April

2020.

[11] Check it out: http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8#sthash.jTiWe8R0.dpuf, http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8, https://ar.wikipedia.org/wiki/Information_production law, https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ for the General Data Protection Regulation: Will it be the standard Global Data Protection?

[12] Engineer / Saeed Attalla, What is the difference between security and privacy, Article published on 14/5/2020 on the site:

https://www.arageek.com/l/whats the difference between security and privacy

[13] HIV.gov, The Difference between Security and Privacy and Why It Matters to Your Program, From the site: www.hiv.govSee it on 7-3-2019

[14] For more on the meaning of privacy, see this:

Osama Ahmed Attalla Is the Legal Protection of Digital Privacy Enough In Egypt "? Protection of Digital Data Privacy ", A Paper Submitted For the Conference of Cyber Crimes, National Institute Of Intellectual Property April 2020.

[15] What's the Difference Between Privacy and Security? , From the site: www.globalsign.comSee it on 7-3-2019

[16] Difference Between Security and Privacy from: www.differencebetween.netSee it on 7-3-2019

[17] Digital Privacy Legislation /https://sitcegypt.org/?p=1425

[18] Check it out: www.dlapiperdataprotection.com. Data Protection Laws of the World

[19] Check it out: www.dlapiperdataprotection.com. Data Protection Laws of the World

[20] Dr. Khalil Khairallah, organizing the electronic medical file and protecting its data in the framework of developing the health sector and health services. DOSSIER MÉDICAL ELECTRONIQUE Posted on:

https://www.lita-lb.org/archive/51-dossier-médical-Electronique.html

Last entry date: 6/29/2020.

[21] Décret n ° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires)

[22] Loi informatique et libertés codifiée par la loi n°2004-801 du 6 aout 2004 pour l'harmonization avec la directive européenne .

[23] Code de la Santé Publique , dernière modification: 1 juillet 2014

[24] https://sitcegypt.org/?p=1425 Digital Privacy Legislation /

[25] International Covenant on Civil and Political Rights- Article 17 .

[26] Convention for the Protection of Human Rights and Fundamental Freedoms

[27] Check it out: https://hi-in-ksa.com/2015/12/20 / data-scientific-databases-magazines-in-the-information/,https://aitnews.com/2018/05/27/General-Regulations-for-data-protectiongdpr/,
http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8#sthash.jTiWe8R0.dpuf,
http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8,
Https://ar.wikipedia.org/wiki/Qanon__khasusih_amuallomat,
https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/depending for the General Data Protection Regulation: Will it be the standard Global Data Protection?
[28] Data Protection Laws of the World, March 2013
[29] Personal Data Protection Act 2012 - REPUBLIC OF SINGAPORE
[30] FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers
[31]https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ for the General Data Protection Regulation: Will it be the global standard for data protection?
[32] Gramm-Leach-Bliley Act - Bureau of Consumer Protection
[33] Children's Online Privacy Protection Act of 1998
[34] FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers - Federal Trade Commission.
[35] Cyber security points Cyber security to methods intended to detect and prevent attacks on any computer system and the information contained therein or unauthorized access. Cyber security aims to protect data or any form of digital asset stored on the computer of any party or any device that contains digital memory.
[36] https://taqadom.aspdkw.com/ Security-Health-Information/
[37] Identifiable data is defined as information that uniquely identifies an individual when used alone or when used in conjunction with other information, and includes personal health information. Privacy is based on a set of foundational principles known as fair principles for informational practices (FIPPs).